Survival in a World of Zero Trust

Survival in a World of Zero Trust

Try the following Thought Experiment. Take 100 random users, put them in a room, and ask them to log into your favorite federated web app. If you tell them to first go create an account with some IdP of Last Resort, they will probably groan and quite likely not grok the value of what you are trying to demonstrate. Indeed.

Instead tell them to choose their favorite social IdP on the discovery interface. This will immediately win over a sizable proportion of your audience who will blithely log into your app with almost zero effort (since most social IdPs will happily maintain a user session indefinitely).

However, as Jim Fox demonstrated on the social identity mailing list the other day, not all users feel comfortable performing a federated login at a social IdP. Some users have a healthy distrust for social IdPs, and moreover, that lack of trust is on the rise. So be it.

What can we conclude from this Thought Experiment? Here's my take. Bottom line: *Federation is Hard*. By no means is the Federated Model a done deal. It may or may not survive, and moreover, I can't predict with any accuracy what *will* prevail.

That said, I *believe* in the Federated Model and I *want* it to work in the long run, so here's what I think we should do in the short term. The appearance of social IdPs on the discovery interfaces of Federation-wide SPs is an inevitability. The sooner we do it, the better off we as users will be. For some (many?), this will simplify the federation experience, and we dearly need all the simplification we can get.

We don't need any more IdPs of Last Resort in the wild, at least not until the trust issues associated with IdPs have been worked out. I'm talking of course about multifactor authentication, assurance, user consent, and privacy, all very hard problems that continue to impede the advance of the Federated Model. In today's atmosphere of Zero Trust, it makes absolutely no sense to keep building and relying on password-based SAML IdPs. That elusive *One IdP That Rules Them All* simply doesn't exist. We need something better. Something that's simple, safe, and private.

If you're still reading this, you'll want to know what the viable alternatives are. Honestly, I don't know. All I can say is that I'm intrigued by the user centric approaches of the IRMA project and the FIDO Alliance. If similar technologies were to proliferate, it would be a death knell for the centralized IdP model. In its place would rise the Attribute Authority, and I don't mean the SSO-based AAs of today. I mean standalone AAs that dish out attribute assertions that end users control. This is the only approach I can see working in a World of Zero Trust.